

# Accelerate Network Operations Efficiency With AIOps

## Table of Contents

Executive Summary	3
Introduction	6
Challenge 1: Disjointed Consoles	6
Solution: Observe	6
Challenge 2: Slow Response	7
Solution: Correlate	7
Challenge 3: Manual Operations	7
Solution: Rapidly Respond and Improve Efficiency	7
Simplify Operations With AIOps Network Operations	8



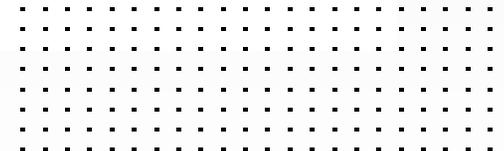
## Executive Summary

For organizations to succeed in their digital transformation, network teams need to make sure that users have a quality experience using any application from anywhere. Fortinet simplifies network operations with comprehensive monitoring and automation that takes advantage of years of experience building artificial intelligence (AI) and machine learning (ML) models that are used by thousands of enterprises globally. No matter how large or small the network operations team may be, challenges arise from complexity related to disjointed consoles, slow responses, and manual operations. Fortinet AIOps Network Operations can help with all three of these challenges.



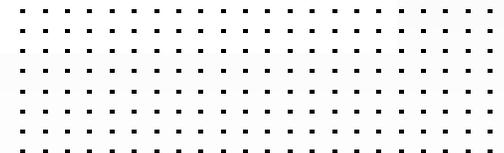


**IDC predicts that by 2023 more than 50% of new IT infrastructure deployments will be at the edge, creating new network environments that will need to be managed and secured.<sup>1</sup>**





**According to Gartner, by 2024, 50% of network operations teams will be required to rearchitect their network monitoring stack, due to the impact of hybrid networking, which will be a significant increase from 20% in 2019.<sup>2</sup> And by 2023, the use of NetOps 2.0 principles will grow by 40%, and those embracing these principles will reduce their application delivery times by 25%.<sup>3</sup>**



# Introduction

Many network operations teams are going through digital transformation projects that are driven by hybrid work environments and the need for digital experience visibility and control that spans from users to applications. Network teams face three key operational challenges and Fortinet can help proactively address each of them with AIOps Network Operations. It improves visibility, reduces mean time to incident (MTTI) detection, and increases incident response efficiency.

## Challenge 1: Disjointed Consoles

Enterprises with distributed edges often deploy multiple point solutions. For example, they might have one solution for wireless in each location, another solution for switching, and another one for network access control. Having solutions from different vendors is challenging especially in manufacturing

environments because operators have to use multiple consoles to operate the networks. The visibility across these disparate consoles is not integrated, so operators can't see a complete picture of what is happening on the network.

## Solution: Observe

Fortinet solutions provide coverage across local-area network (LAN), wide-area network (WAN), and cloud, and with AIOps Network Operations, you can understand the performance and security anomalies all the way from user to application access. Simplifying monitoring across wireless, switch, firewall, software-defined WAN (SD-WAN), secure access service edge (SASE) into one console makes it easier for operations staff to ensure users have a good experience no matter where they may be connecting on the network.



## **Challenge 2: Slow Response**

Performing root cause analyses (RCA) to track down user experience issues in a multilayered, distributed, and complex network is not a trivial exercise. It can take time to resolve issues.

### **Solution: Correlate**

Fortinet AIOps Network Operations analyzes the dependence of device, LAN, WAN, and cloud events. At the same time, it incorporates policies to identify the root causes of end-user performance issues. Teams can more easily cut through the noisy events and find the issues that are affecting the business.

## **Challenge 3: Manual Operations**

Spending time performing manual operations limits an operator's ability to predict and remediate user experience issues.

### **Solution: Rapidly Respond and Improve Efficiency**

By integrating security orchestration, automation, and response (SOAR) into network operations, organizations can unlock enterprise network automation both proactively and through rules that use AI/ML and automation to remediate issues before they arise.



# Simplify Operations With AIOps Network Operations

Fortinet AIOps Network Operations provides proactive visibility and control for heterogeneous and distributed networks. Designed for enterprises and service providers, it offers:

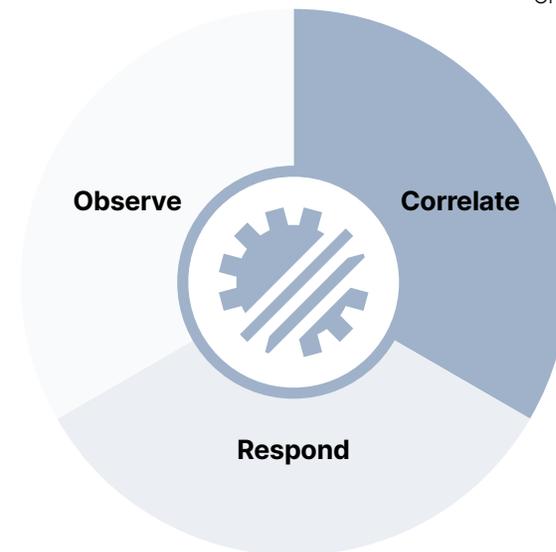
- **Hybrid-IT network visibility.** Improve visibility with a unified console for measuring digital experience key performance indicators across your enterprise network, instead of going to multiple consoles and stitching the information together.
- **User experience performance RCA.** Improve the MTTI a root cause for an incident when there is a user experience issue on the network, whether it is attributed to LAN, WAN, device, or an application in the end-to-end access path.
- **AI-powered network incident response.** Improve the mean time to resolve (MTTR) issues with intelligent and proactive response actions for network operations teams with self-healing capabilities across all of the distributed edges of the network.



- Network monitoring
- Anomaly detection
- Troubleshooting analytics



- WAN, LAN, firewall correlation
- Incident triage automation
- Change management



- 300+ out-of-box playbooks
- Integrated workflow engines
- NetOps scripts

Figure 1: AIOps network operations.

<sup>1</sup> Frank Gens, et al., "[Worldwide IT Industry 2020 Predictions](#)," IDC FutureScape, October 2019.

<sup>2</sup> Josh Chessman, "[Market Guide for Network Performance Monitoring and Diagnostics](#)," Gartner, March 5, 2020.

<sup>3</sup> Josh Chessman, et al., "[NetOps 2.0: Embrace Network Automation and Analytics to Win in the Era of ContinuousNext](#)," Gartner, October 9, 2019.



[www.fortinet.com](http://www.fortinet.com)

Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.